Smart Card

Secret Key

Plaintext → Encryption → Ciphertext

FIG. 1

PRIOR ART

K_i

X_i ——→ $(+)$ ——→ Z_i

XOR
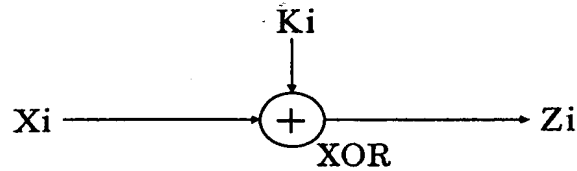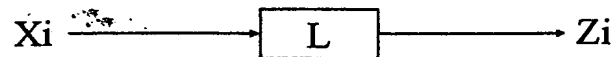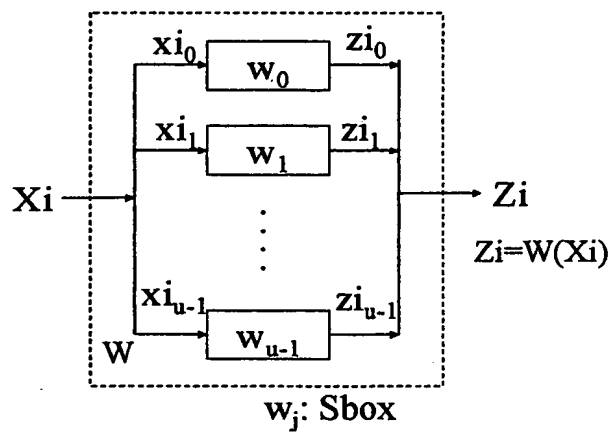
FIG. 2

PRIOR ART

X_i ——→ L ——→ Z_i

FIG. 3

PRIOR ART
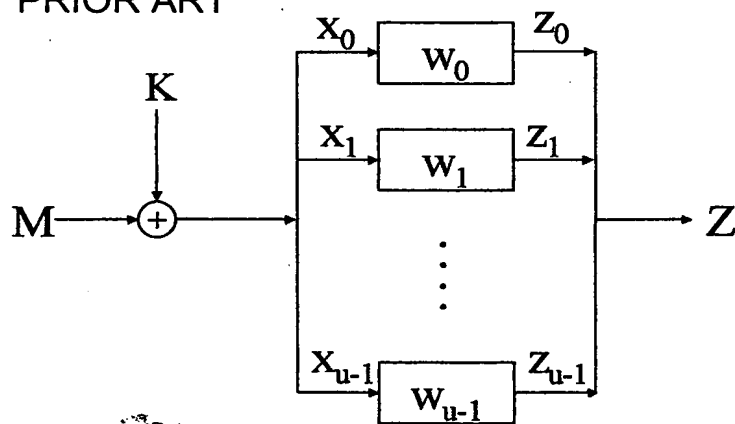
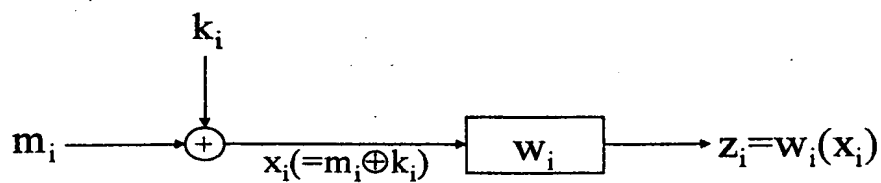# FIG. 4

PRIOR ART

FIG. 5

PRIOR ART

FIG. 6

PRIOR ART

FIG.7A

PRIOR ART

Voltage

Time

FIG.7B

PRIOR ART

Voltage

Time

FIG.7C

PRIOR ART

Voltage

Time

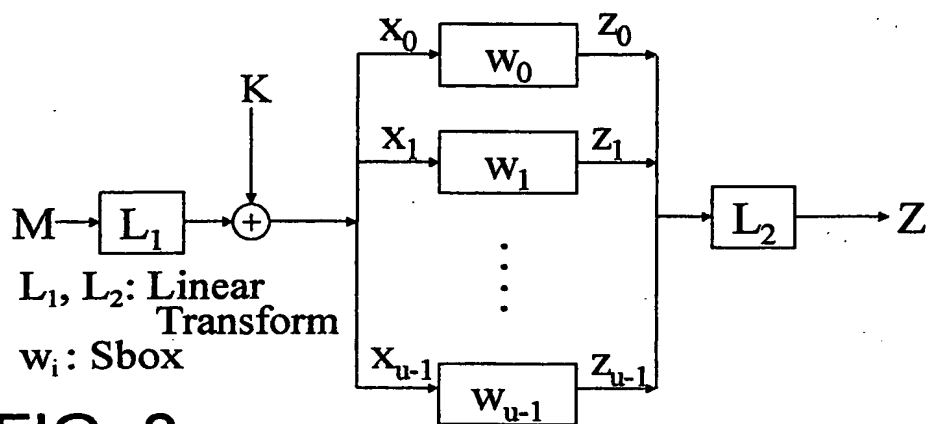**FIG.7D**

PRIOR ART

Voltage

Time
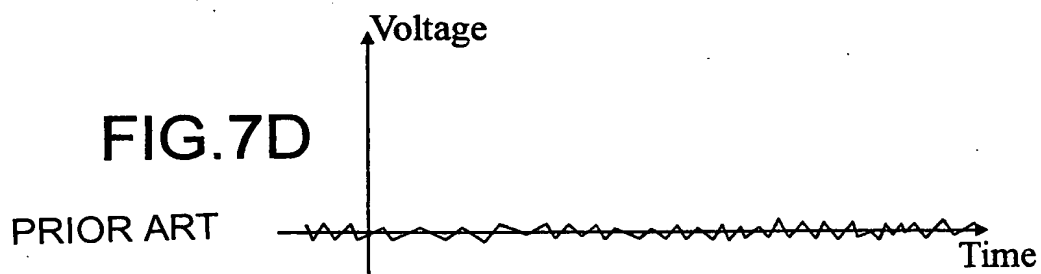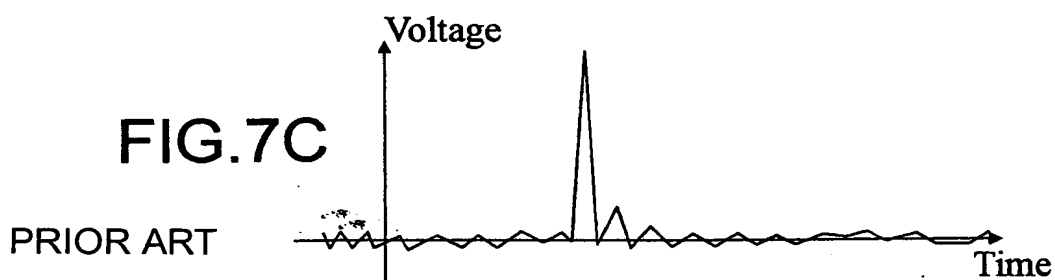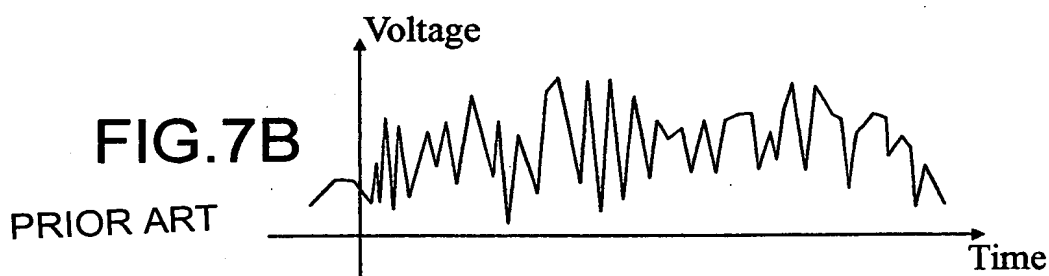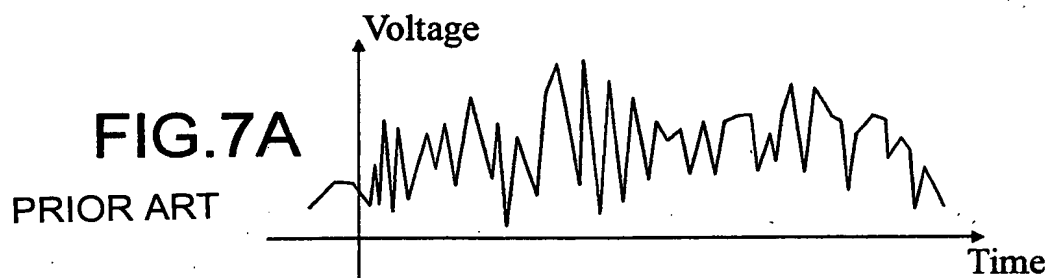
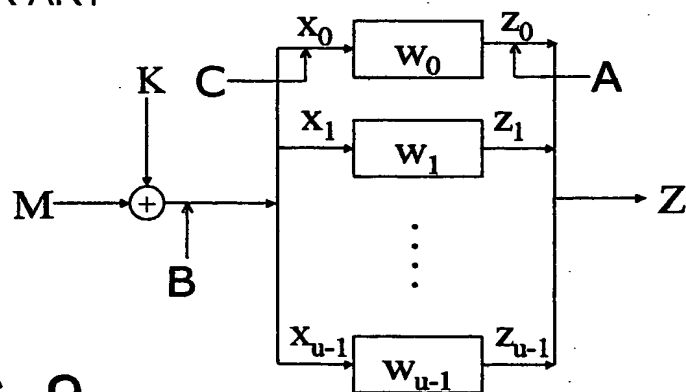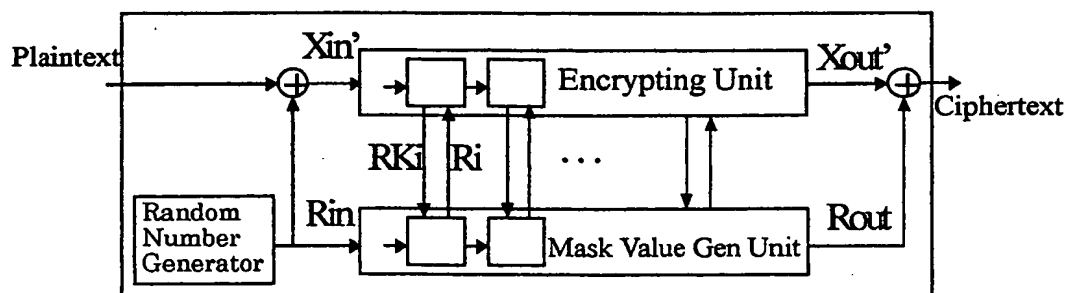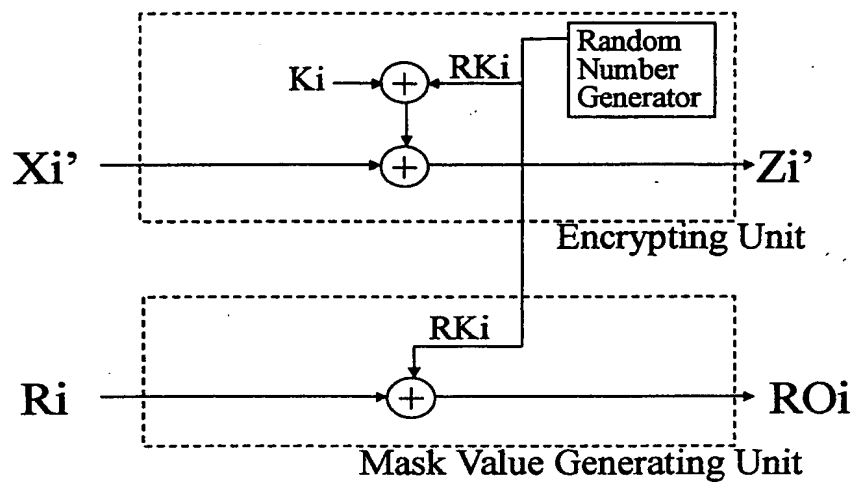## FIG. 8

PRIOR ART

FIG. 9

PRIOR ART

FIG. 10

PRIOR ART

Key XOR in Random Mask Value Method
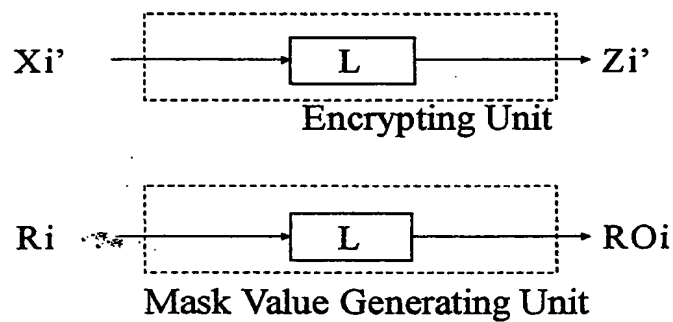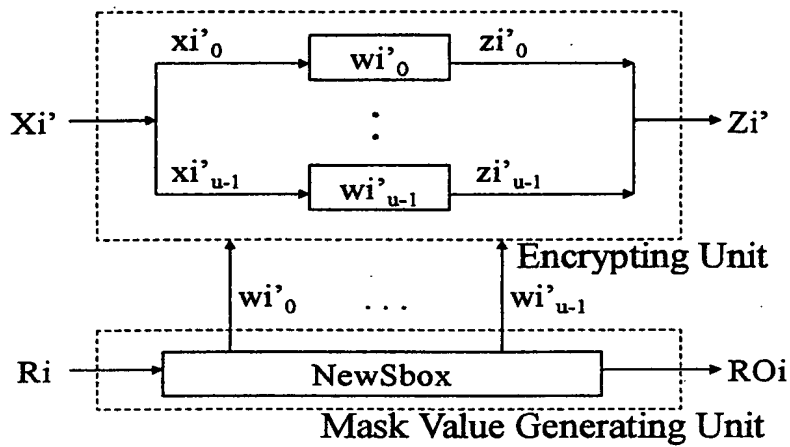
FIG. 11

PRIOR ART

FIG. 12

PRIOR ART

FIG. 13A
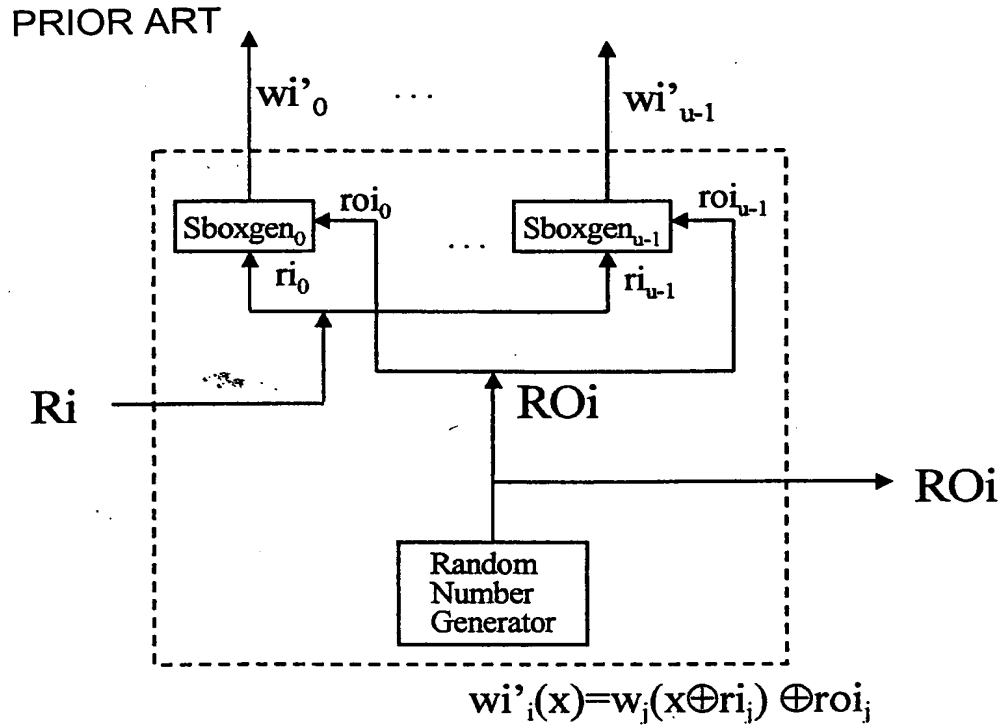
$$wi'_i(x) = w_j(x \oplus ri_j) \oplus roi_j$$

FIG. 13B

Conventional Rijndael Encryption

FIG. 14

PRIOR ART

K_{sec} $\longrightarrow$ Sub-key Generator $\longrightarrow$ $K_0, K_1, \ldots, K_N$

(128/192/256-Bit Secret Key)   (N+1 Sub-keys)

Generation of Sub-keys in Rijndael Encryption

FIG. 15

PRIOR ART

$y_i = S(x_i)$

Subbyte

FIG. 16

PRIOR ART

$y_i = x_j,$
$j = 13i - 4 \pmod{16}$

Shift

FIG. 17

PRIOR ART

$$\begin{pmatrix} y_{4i+3} \\ y_{4i+2} \\ y_{4i+1} \\ y_{4i} \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} x_{4i+3} \\ x_{4i+2} \\ x_{4i+1} \\ x_{4i} \end{pmatrix}$$

Modulo Arithmetic for
Irreducible Polynomial
$x^8+x^4+x^3+x+1$ over $GF(2^8)$

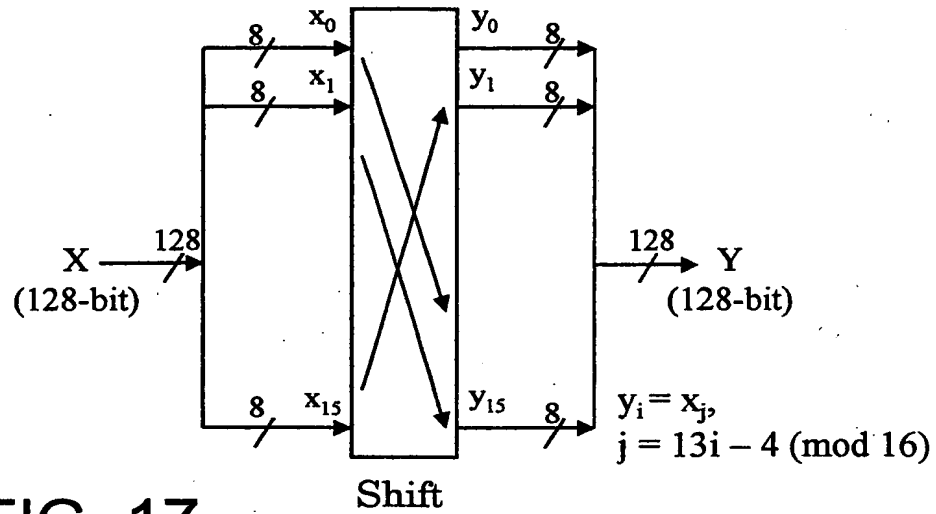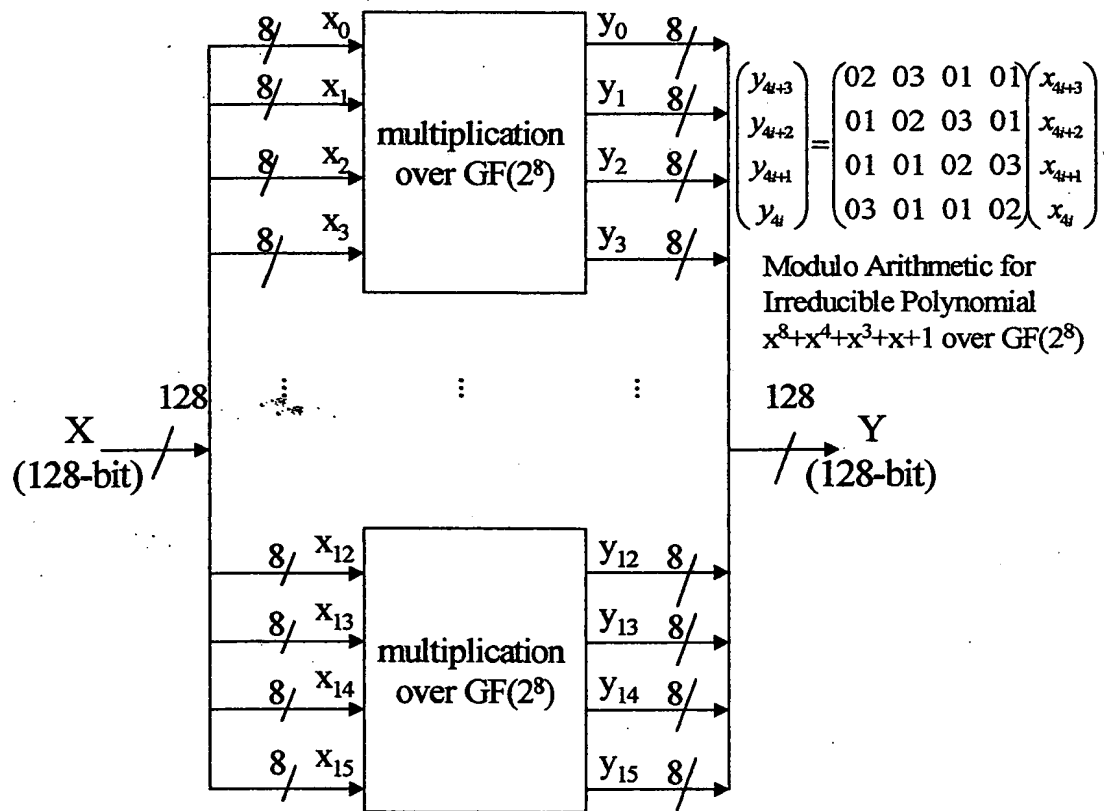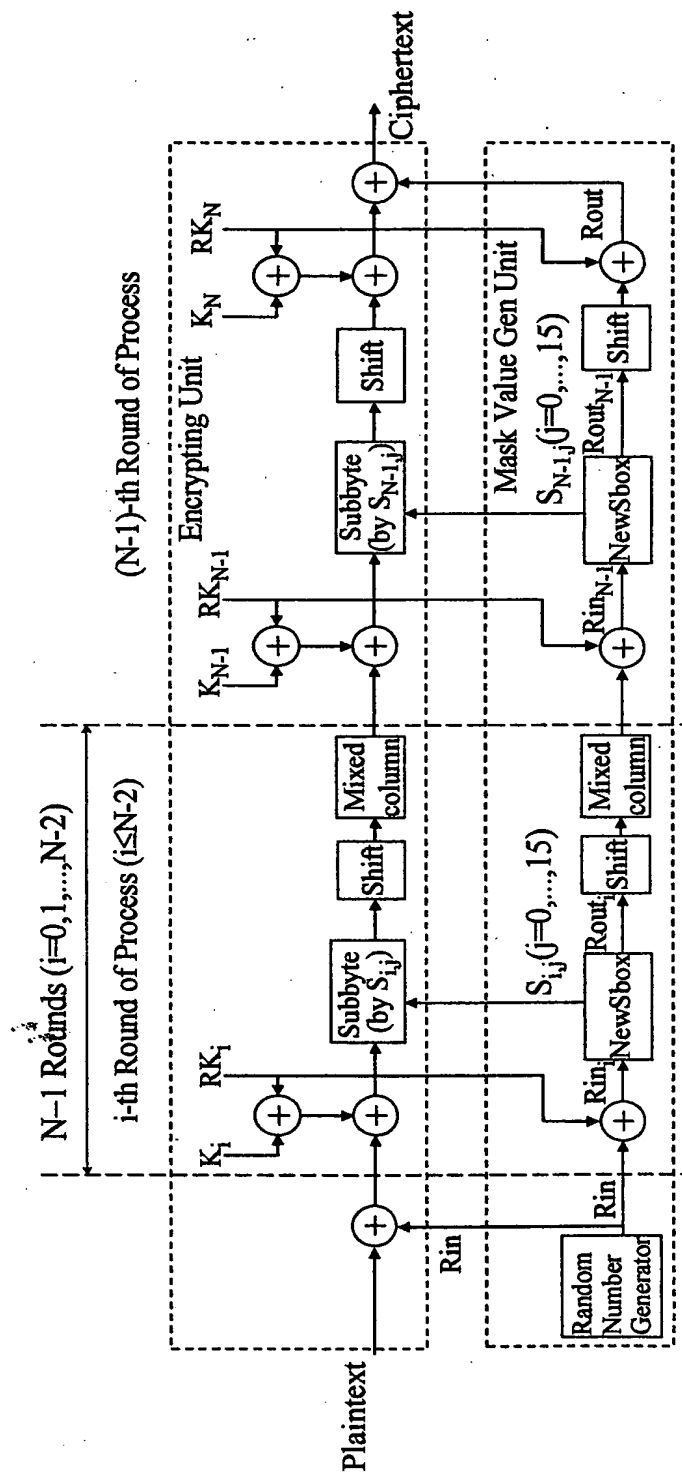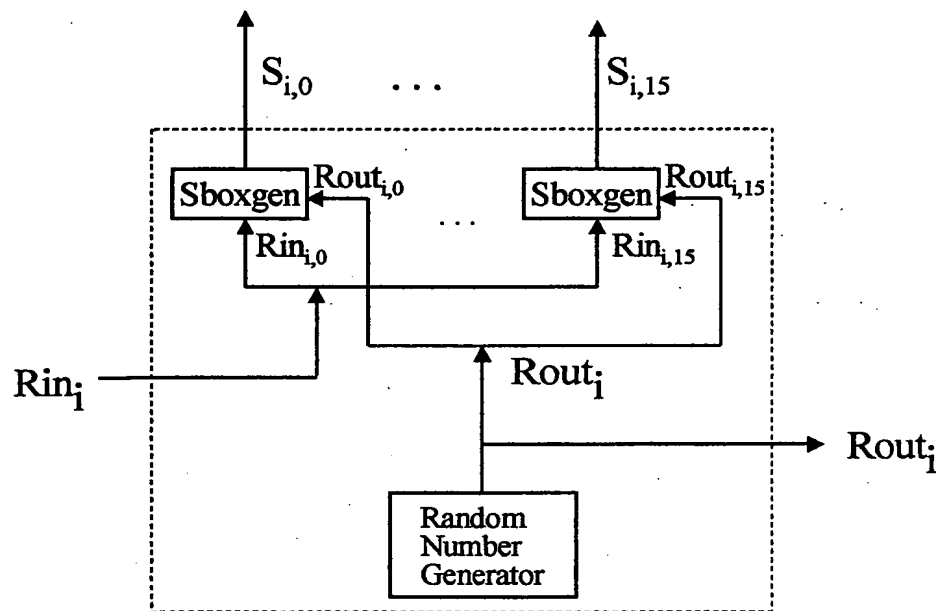# FIG. 18

Mixedcolumn
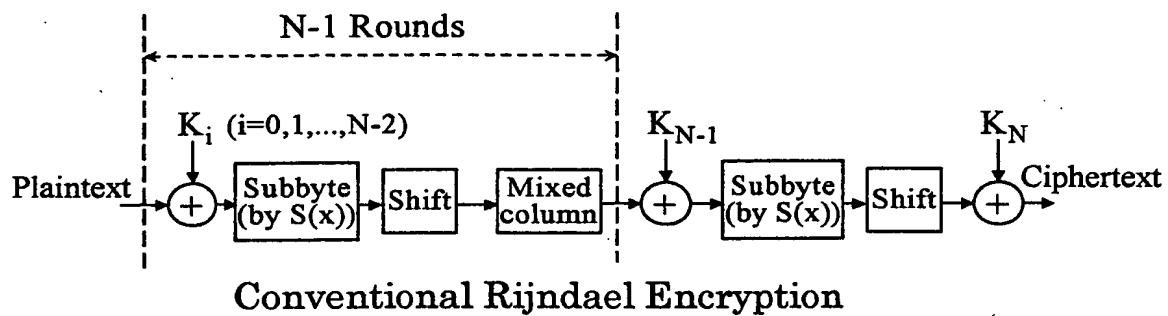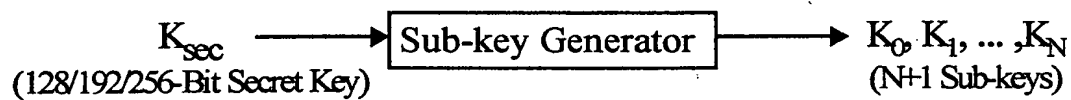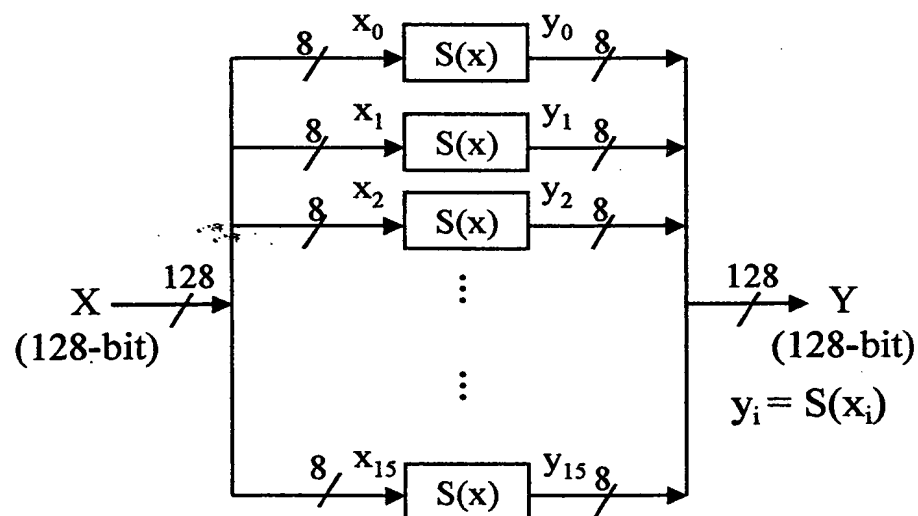
PRIOR ART

FIG. 19

PRIOR ART

Sboxgen Generates Sbox, $S_{i,j}$, such that $S_{i,j}(x) = S(x \oplus Rin_{i,j}) \oplus Rout_{i,j}$

NewSbox

FIG. 20

PRIOR ART